AMENDMENTS TO THE CLAIMS

1-8 (Canceled)

9. (Currently Amended) A data transfer system comprising:

a key facility;

a sender facility ~~configured to communicate~~for communicating with the key facility, the sender facility comprising:

a first encryption module ~~configured to encrypt~~for encrypting data for an intended recipient, wherein a first encrypted part and a remaining encrypted part are produced, the first encrypted part carrying information for decryption of the remaining encrypted part such that the remaining encrypted part can be decrypted only after decrypting the first encrypted part;

a second encryption module ~~configured to encrypt~~ for encrypting the first encrypted part so as to produce a third encrypted part;

a combiner ~~configured to combine~~for combining the third encrypted part with the remaining encrypted part to produce a data block, and

a first transmitter ~~configured to send~~ for sending the data block; and

a receiver facility ~~configured to communicate~~ for communicating with the key facility, the receiver facility comprising:

a receiver ~~configured to receive~~for receiving the data block;

a splitter ~~configured to split~~for splitting the data block into the third encrypted part and the remaining encrypted part; and

a command module ~~configured to generate~~ for generating a request for the key facility to recover the first encrypted part by decrypting the third encrypted part, wherein the receiver is ~~further configured to receive~~ also for receiving the first encrypted part from the key facility;

wherein the key facility further comprises:

a first decryption module ~~configured to recover~~ for recovering the first encrypted part by decrypting the third encrypted part after receipt of the request from the receiver facility and after receipt of the third encrypted part; and

a second transmitter ~~configured to send~~for sending the first encrypted part to the receiver facility,

wherein the receiver facility further comprises a second decryption module ~~configured to enable~~ for enabling subsequent decryption of the remaining encrypted part by decrypting the first encrypted part.

10. (Previously Presented) The system of Claim 9, wherein the sender facility includes a signature module to sign the data block.

11. (Previously Presented) The system of Claim 9, wherein the first transmitter is configured to send the data block to the key facility, and wherein the key facility further includes a receiver configured to receive the data block and to forward the data block to the receiver facility.

12. (Previously Presented) The system of Claim 11, wherein the key facility further includes a log module configured to log receipt of the data block.

13. (Previously Presented) The system of Claim 9, wherein the receiver facility is configured to communicate with the key facility and the sender facility, and wherein the first transmitter is configured to send the data block to the receiver facility, the receiver facility further comprising a receiver to receive the data block.

14. (Previously Presented) The system of Claim 13, wherein the key facility further comprises a log module configured to log receipt of the third encrypted part.

15. (Previously Presented) The system of Claim 9, wherein the key facility further comprises a log module configured to log receipt of the request for decryption of the third encrypted part as proof of delivery of the data block to the receiver facility.

16. (Previously Presented) The system of Claim 15, wherein the sender facility further comprises a delivery module configured to request proof of delivery information from the key facility.

17. (Previously Presented) The system of Claim 9, wherein the key facility is a trusted third party.

18. (Previously Presented) A method of data transfer, comprising:

at a sender facility, encrypting data for an intended recipient, wherein a first encrypted part and a remaining encrypted part are produced, the first encrypted part carrying information for decryption of the remaining encrypted part, wherein the remaining encrypted part can be decrypted only after decrypting the first encrypted part;

at the sender facility, encrypting the first encrypted part to produce a third encrypted part;

at the sender facility, combining the third encrypted part with the remaining encrypted part to produce a data block, and

at the sender facility, sending the data block;

at a receiver facility, receiving the data block;

at the receiver facility, splitting the data block into the third encrypted part and the remaining encrypted part; and

at the receiver facility, generating a request for a key facility to decrypt the third encrypted part;

at the key facility, recovering the first encrypted part by decrypting the third encrypted part after receipt of the request from the receiver facility and after receipt of the third encrypted part;

at the key facility, transmitting the first encrypted part to the receiver facility;

at the receiver facility, receiving the first encrypted part from the key facility;

at the receiver facility, enabling subsequent decryption of the remaining encrypted part by decrypting the first encrypted part; and

at the receiver facility, decrypting the remaining encrypted part.

19. (Previously Presented) The method of Claim 18, further comprising signing the data block at the sender facility.

20. (Previously Presented) The method of Claim 18, wherein the sending at the sender facility comprises sending the data block to the key facility, and wherein the method further comprises at the key facility receiving the data block and forwarding the data block to the receiver facility.

21. (Previously Presented) The method of Claim 20, further comprising, at the key facility, logging receipt of the data block.

22. (Previously Presented) The method of Claim 18, wherein the sending at the sender facility comprises sending the data block to the receiver facility, and wherein the method further comprises, at the receiver facility, receiving the data block.

23. (Previously Presented) The method of Claim 22, further comprising, at the key facility, logging receipt of the third encrypted part.

24. (Previously Presented) The method of Claim 18, further comprising, at the key facility, logging receipt of the request for decryption of the third encrypted part as proof of delivery of the data block to the receiver facility.

25. (Previously Presented) The method of Claim 24, further comprising, at the sender facility, requesting proof of delivery information from the key facility.

26. (Previously Presented) The method of Claim 18, wherein the key facility is a trusted third party.

27. (Previously Presented) A data transfer system comprising:

a key facility;

a sender facility configured to communicate with the key facility, the sender facility comprising:

a first encryption module configured to encrypt data for an intended recipient;

a partitioning module configured to split the data into a plurality of encrypted parts such that no part is decryptable on its own;

a second encryption module configured to produce a further encrypted part for the key facility by encrypting at least one of the encrypted parts;

a combiner configured to produce a data block by combining the further encrypted part and at least one other encrypted part;

a signature module configured to sign the data block; and

a first transmitter configured to send the data block to the key facility; and

a receiver facility configured to communicate with the key facility, the receiver facility comprising:

a receiver configured to receive the data block from the key facility; and

a command module configured to generate a request for decryption of the further encrypted part by the key facility;

wherein the key facility comprises:

a receiver configured to receive the data block from the sender facility and to forward the data block to the receiver facility;

a first log module configured to log recipt of the data block from the sender facility;

a second log module configured to log receipt of the decryption request from the receiver facility as proof of delivery of the data block to the receiver facility;

a first decryption module configured to decrypt the further encrypted part after receipt of the request from the receiver facility; and

a second transmitter configured to send the decrypted further encrypted part to the receiver facility,

wherein the receiver facility further comprises a second decryption module configured to decrypt the other encrypted part and the decrypted further encrypted part; and

wherein the sender facility further comprises a delivery module configured to request proof of delivery information from the key facility.

28. (Previously Presented) A data transfer system comprising:

a key facility;

a sender facility configured to communicate with the key facility and a receiver facility, the sender facility comprising:

a first encryption module configured to encrypt data for an intended recipient;

a partitioning module configured to split the data into a plurality of encrypted parts such that no part is decryptable on its own;

a second encryption module configured to produce a further encrypted part for the key facility by encrypting at least one of the encrypted parts;

a combiner configured to produce a data block by combining the further encrypted part and at least one other encrypted part;

a signature module configured to sign the data block; and

a first transmitter configured to send the data block to the receiver facility,

wherein the receiver facility is configured to communicate with the key facility and the sender facility, and the receiver facility comprises:

a receiver configured to receive the data block from the sender facility; and

a command module configured to generate a request for decryption of the further encrypted part by the key facility,

wherein the key facility further comprises:

a log module configured to log receipt of the further encrypted part;

a first decryption module configured to decrypt the further encrypted part after receipt of the request from the receiver facility and after receipt of the further encrypted part; and

a second transmitter configured to send the decrypted further encrypted part to the receiver facility; and

wherein the receiver facility further comprises a second decryption module configured to decrypt the other encrypted part and the decrypted further encrypted part received from the key facility.

29. (Previously Presented) A method of transferring data, comprising:

at a sender facility, encrypting data for an intended recipient, splitting the data into encrypted parts such that no part is decryptable on its own, producing a further encrypted part by encrypting at least one of the encrypted parts for a key facility, producing a data block by combining the further encrypted part and a remaining encrypted part, signing the data block, and sending the data block to the key facility;

at the key facility, receiving the data block from the sender facility, forwarding the data block to a receiver facility, and logging receipt of the data block from the sender facility;

at the receiver facility, receiving the data block from the key facility, and generating a request for decryption of the further encrypted part by the key facility;

at the key facility, logging receipt of the decryption request from the receiver facility as proof of delivery of the data block to the receiver facility, decrypting the further encrypted part after receipt of the request from the receiver facility, and sending the decrypted further encrypted part to the receiver facility;

at the receiver facility, decrypting the decrypted further encrypted part and the other encrypted part received from the key facility; and

at the sender facility, requesting proof of delivery information from the key facility.

30. (Canceled)